(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2002 (27.06.2002)

PCT

(10) International Publication Number
WO 02/51096 A1

(51) International Patent Classification[7]: H04L 29/06, H04N 7/167

(21) International Application Number: PCT/IB01/02406

(22) International Filing Date:
10 December 2001 (10.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00204639.9 18 December 2000 (18.12.2000) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: VAN RIJNSOEVER, Bartholomeus, J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; International Octrioobureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

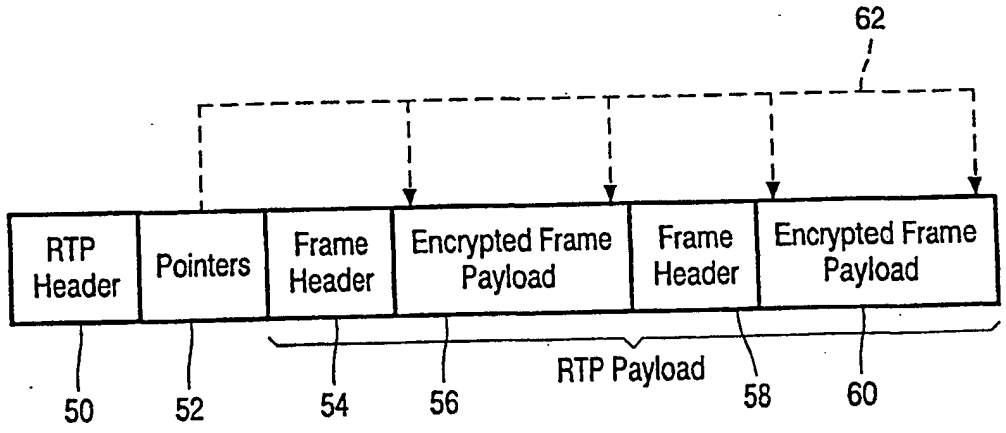
(81) Designated State *(national)*: JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: POINTERS TO ENCRYPTED DATA IN RTP HEADER



(57) Abstract: Frame-formatted user data is real-time transmitted whilst thereon effecting before transmission a frame-based encryption procedure. In particular, before subjecting to the encryption procedure, localizing data is joined to the data frame and placed into predetermined governance locations that are excluded from the subsequent encrypting.

WO 02/51096 A1

Pointers to encrypted data in RTP header

A method and system for real-time transmitting frame-formatted user data through joining thereto frame localizing data placed in predetermined governance locations, whilst before transmission effecting an encryption procedure that excludes said localizing data, and a system, a transmitter apparatus, a receiver apparatus, and a signal produced by such transmitter apparatus for use with such method.

BACKGROUND OF THE INVENTION

The invention relates to a system as recited in the preamble of Claim 1. Data, and in particular, but not restricted to, multi-media data are at present being encrypted for implementing inter alia various conditional access schemes to allow creators and distributors of the original matter to collect an appropriate amount of retributions from users of such information. At the receiver side, the user data must be recuperated in order to allow for orderly representing, viewing, listening, executing, and other user-associated operations. The actual transmission via some transmission medium, such as a network, will take place on a packetized level, where the packets are standardized for the network or networks in question.

A first approach is to effect the encryption on the basis of a Real Time Protocol transmission packet, which is a relatively simple procedure and is alright for protecting the transmission proper. Alternatively, a higher protection level can be attained that will also remain in force at the receiver side: this can be done by having the encryption implemented on the basis of the frame structure of the source data or user data. It is also feasible to implement a combination of the two above approaches. Now, the encryption should advantageously be executed in a standard component that should not need to effect complicated preprocessing to find the start of a frame. Therefore, all of the above procedures will need an easy mechanism to straightforwardly find the beginning of the frames.

SUMMARY TO THE INVENTION

In consequence, amongst other things, it is an object of the present invention to add specific localizing information to allow the encoder mechanism and possibly, also the decoder mechanism to quickly and easily find the start of the various frames.

Now therefore, according to one of its aspects the invention is characterized according to the characterizing part of Claim 1.

Further to the above, the present inventor has recognized that a slight modification to the above may allow to have only a part of the user data being effectively encrypted, whilst still enabling the immediate localizing of the various such encrypted parts, as has been recited in Claim 2. The invention also relates to a system being arranged for implementing the method as claimed in Claim 1, to a transmitter apparatus and to a receiver apparatus for use in such system, and to a signal produced by such transmitter apparatus. Further advantageous aspects of the invention are recited in dependent Claims.

BRIEF DESCRIPTION OF THE DRAWING

These and further aspects and advantages of the invention will be discussed more in detail hereinafter with reference to the disclosure of preferred embodiments, and in particular with reference to the appended Figures that show:

Figure 1, a system arranged for implementing the inventive method;

Figure 2, a data format implementation for use in the present invention;

Figure 3, an amended format with respect to Figure 2 that has partial encrypting.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The quality of content information, such as audio or video on the Internet is improving due to steady advances in coding technology and in transmission bandwidth. Content providers intend to sell such high value content, and therefore, a need is arising for effecting conditional access or digital rights management, as it is called. Such conditional access system will encrypt a content item and will subsequently manage the associated decryption keys in such manner that only authorized end users will be able to decrypt and thereby reconstitute the original content in full.

Now, multi-media data is generally structured in frames, wherein the size of a frame is related to the category of information. Furthermore, the size of a transmitted frame may

relate to the degree of compaction and other processing it has been subjected to before encryption. In fact, the frames may be larger as well as smaller than the packets used for actual transmission. Therefore, a single transmission packet may contain one or more frames, or fractional parts of a frame. ***Streaming*** is a technology wherein a client will play or otherwise use the content as soon as it will arrive, so there will be no downloading of all, or a substantial part of, an entire content before playing. Streaming will not allow for retransmission of packets. The content user will have to cope with the occurrence of lost data.

Now for optimum protection, content is best encrypted at the frame level, even with non-uniform frame size. Such encryption at the frame level will allow for persistent or end-to-end encryption that applies to both transmitted as well as to stored content. Preferably, the system component that implements the actual encryption is a generic component, and should therefore be independent of specific streaming servers and independent of specific frame formats. One way to achieve this is to define the encryption component as a Realtime-Transmission-Protocol- or RTP-translator. At present, virtually all streaming servers are using the RTP streaming protocol. Therefore, the encryption component could receive the RTP packets, encrypt the payload, and subsequently forward the encrypted RTP packets. Alternatively, the encryption may be integrated with the streaming server.

Alternatively, the encryption may be executed on the level of the RTP-packet. This will protect the transmission proper, whilst surrendering part of the protection at the receiver side after receiving. Also, a combination of these two encryption approaches is feasible, such as by assigning the appropriate encryption level on the basis of a contingency strategy viz à viz available hardware facilities.

A problem is posed in that the headers of the frames must remain unencrypted, such as when the encryption is effected at the frame level. This requires that the generic encryption component should analyze the payloads of the RTP packets to identify the positions of the frame headers. Such would however lower the performance of the encryption component, and will also make the encryption component dependent on actual frame formats.

The present invention provides a solution to the problem in question by extending the headers of RTP packets to include pointers to those parts of the RTP packet payload that actually need to be encrypted. The pointers are set by the streaming server. The server may do this as part of the so-called hint process, that is an off-line analysis of multi-media data, so that the data may be streamed more efficiently at a later instant in time. The result of the hint process is stored in parallel to the content in a so-called hint track.

Figure 1 illustrates a system arranged for implementing the inventive method. Input 23 receives the user data frames, that are transiently stored into storage 22, which accommodates storage of a plurality of such frames. Processing block 24 thereupon joins to these data frames frame header localizing informations in the context of an RTP packet that may comprise a plurality of such user frames, but not necessarily an integer number thereof. The result of this processing is transiently stored in block 26 that accommodates multiple RTP payloads. For brevity, the specific ***hint*** track mentioned supra has not been shown separately. In fact, the hint track facility will be recognized by persons skilled in the art as a standard facility. In practice, such hint track will be implemented at the input side of block 23 to allow indicating the various frame locations. Before transmission, the user data are encrypted in encryption module 28 and transmitted over communication facility 30, such as Internet. The whole procedure at the transmitter side of the system shown may be synchronized by overall synchronization facility 20 as indicated by dashed lines leading therefrom.

At the receiving side, decryption is effected through decryption facility 34, and the result thereof is transiently stored in block 36. Reconstitution of the user frames is effected in processing facility 38, followed by transiently storing in block 40. User application is then symbolized by block 42. Storage blocks 36, 40 do not accommodate downloading of a complete program or a substantial part thereof, but rather will provide for some synchronizing to cater for transfer speed variations of communication facility 30. Again, at the receiver side, overall synchronization is effected through synchronizer block 32.

Figure 2 illustrates an exemplary data format implementation for use in the present invention. For brevity, only a single implementation has been shown. Various data blocks 50-60 of the RTP configuration have been shown in the Figure. Of these, blocks 54-60 constitute the RTP payload, wherein blocks 56, 60 each contain an encrypted frame payload, and blocks 54, 58 contain the associated frame headers. Note that the lengths of blocks 56, 60 need not be uniform. Block 50 contains an RTP header, and is followed by block 52 that contains pointers. As shown in the figure, the pointers 62 indicate both the beginning and the end of each encrypted frame payload. Now, the header 50 is found in the hint track; pointers 52 are extensions of the RTP header 50. This hint track is used by the streaming server for packaging the RTP packets.

Figure 3 illustrates an amended format with respect to Figure 2 that has partial encryption of the user data. For brevity, only the aspects that differentiate from Figure 2 have been indicated specifically. Within the frame payload, the discrimination between encrypted (E) and unencrypted user data has been indicated by a slanted line. The localizing information

indicated by 62 in this case will now specifically indicate (63, 65) the ends of the respective encrypted parts, assuming that the encryption starts from the beginning of the frame's user data. Of course, other partial encryptions may be used. The encryption itself may be done on the level of a frame or partial frame, on the level of a packet, or be based on a combination thereof.

CLAIMS:

1. A method for real-time transmitting or retransmitting frame-formatted user data whilst thereon effecting before such (re-)transmitting an encryption procedure,

said method being characterized by the step of, associated to subjecting said user data to said encryption procedure, joining to said user data appropriate frame localizing data and placing such frame localizing data into predetermined governance locations which, just as well as header informations, are excluded from subsequent said encryption procedure.

2. A method as claimed in Claim 1, whilst subjecting only a part of said user data to said encryption procedure whilst providing for encryption localizing data in said governance locations to discriminate between encrypted and non-encrypted parts of said user data.

3. A method as claimed in Claim 1 or 2, wherein such governance locations are header extension information locations.

4. A method as claimed in Claim 1 or 2, wherein said user data after encryption are transmitted in RTP-packets, and wherein said user data are encrypted on a level of said RTP packet.

5. A method as claimed in Claim 1 or 2, wherein said user data are encrypted on a frame level.

6. A method as claimed in Claims 4 or 5 wherein said transmission allows for imparting partial frames to a packet, as well as allowing to impart a plurality of frames to a single packet.

7. A method as claimed in Claim 3, wherein such header extension information location has a plurality of frame localizing data.

8. A method as claimed in Claim 1 or 2, wherein such governance locations are placed within a separate hint track.

9. A system arranged for implementing a method as claimed in Claim 1 and having transmission means for real-time transmitting or retransmitting frame-formatted user data and encryption means for effecting before such (re-)transmitting an based encryption procedure on said user data,

said system being characterized by comprising next to said encryption means joining means for joining to said user data frame localizing data and placing such frame localizing data into predetermined governance locations which, just as well as header informations, are excluded from subsequent said encryption.

10. A system as claimed in Claim 9, and being arranged for interfacing to Internet as a transmission medium.

11. A transmitter apparatus being arranged for use as a station in a system as claimed in Claim 9.

12. A signal produced by a station as claimed in Claim 11.

13. A receiver apparatus being arranged for use as a station in a system as claimed in Claim 9 and having decryption means for upon reception decrypting user data that had been subject to said encryption procedure for outputting user data so decrypted as based on frames containing said user data.

14. A receiver apparatus as claimed in Claim 13, wherein said decryption means are operational on a frame level.

15. A receiver apparatus as claimed in Claim 13, wherein said decryption means are operational on a packet level.

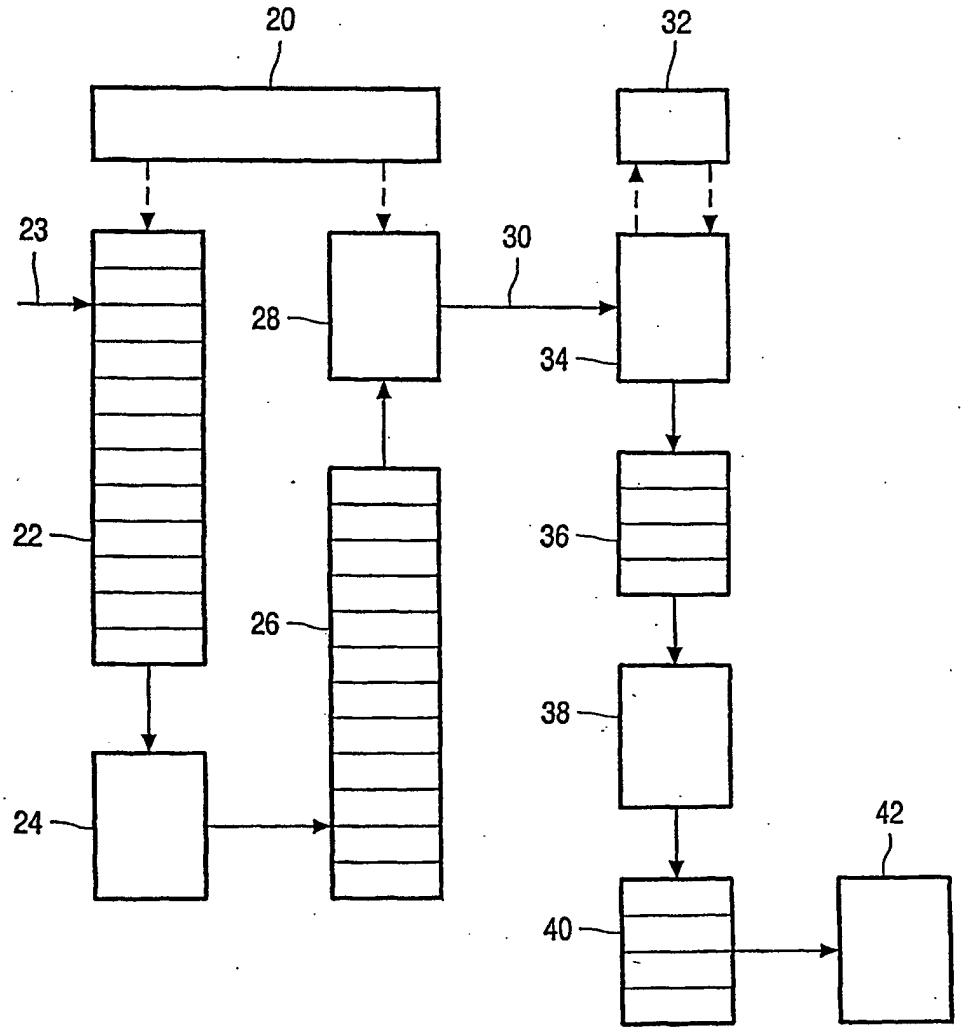


FIG. 1

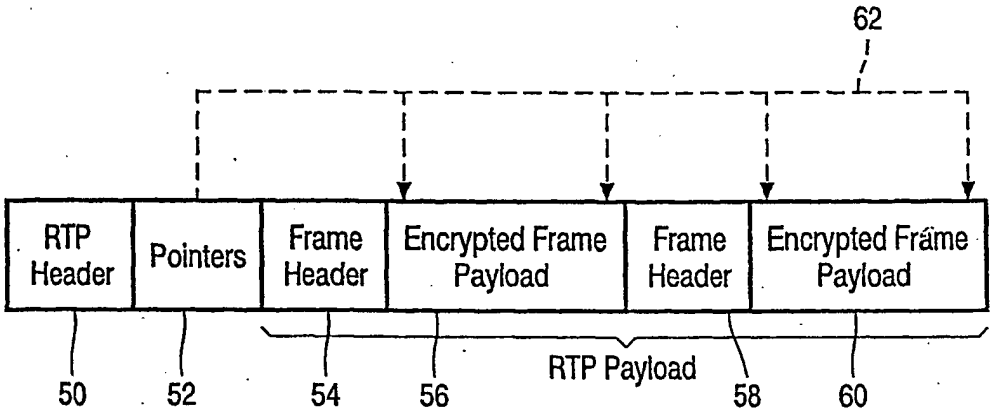

62
RTP Header
Pointers
Frame Header
Encrypted Frame Payload
Frame Header
Encrypted Frame Payload
RTP Payload
50
52
54
56
58
60

FIG. 2

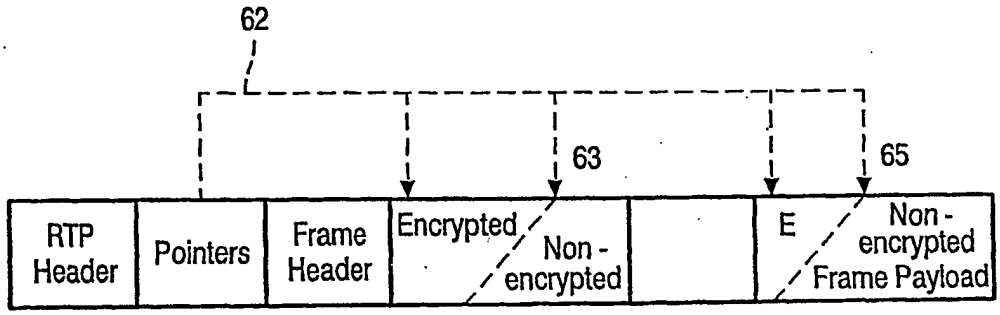

62
63
65
RTP Header
Pointers
Frame Header
Encrypted
Non - encrypted
E
Non - encrypted Frame Payload

FIG. 3

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 37056 A (APPLE COMPUTER) 22 July 1999 (1999-07-22) page 20, line 6 - line 7 page 38, line 9-12	1,9
A	US 5 953 418 A (TAPU MARIAN ET AL) 14 September 1999 (1999-09-14) figure 14	1,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2002	11/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tito Martins, J

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9937056 A	22-07-1999	AU 2232799 A	02-08-1999
		AU 2232899 A	02-08-1999
		AU 2322499 A	02-08-1999
		CA 2316852 A1	22-07-1999
		CA 2318963 A1	22-07-1999
		CA 2325828 A1	22-07-1999
		CN 1308437 A	15-08-2001
		CN 1290444 T	04-04-2001
		CN 1290445 T	04-04-2001
		EP 1051008 A2	08-11-2000
		EP 1048156 A2	02-11-2000
		EP 1062782 A2	27-12-2000
		JP 2002510165 T	02-04-2002
		WO 9937056 A2	22-07-1999
		WO 9937057 A2	22-07-1999
		WO 9937072 A2	22-07-1999
		US 6134243 A	17-10-2000
US 5953418 A	14-09-1999	US 5869279 A	09-02-1999
		WO 9700328 A1	03-01-1997
		US 5770404 A	23-06-1998
		AU 6477596 A	15-01-1997
		CA 2224238 A1	03-01-1997
		EP 0832525 A2	01-04-1998
		WO 9700564 A2	03-01-1997
		US 5802311 A	01-09-1998
		US 5948119 A	07-09-1999

US005805700A

United States Patent [19]

Nardone et al.

[11] Patent Number: 5,805,700

[45] Date of Patent: Sep. 8, 1998

[54] POLICY BASED SELECTIVE ENCRYPTION OF COMPRESSED VIDEO DATA

[75] Inventors: **Joseph M. Nardone**, Portland, Oreg.; **Keith L. Shippy**, Tempe, Ariz.; **David W. Aucsmith**, Portland, Oreg.

[73] Assignee: **Intel Corporation**, Santa Clara, Calif.

[21] Appl. No.: **730,065**

[22] Filed: **Oct. 15, 1996**

[51] **Int. Cl.**[6] **H04N 7/167**

[52] **U.S. Cl.** **380/10**; 380/20

[58] **Field of Search** 380/20, 10

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,515,437	5/1996	Katta et al.	380/20
5,594,492	1/1997	O'Callaghan et al.	380/20
5,617,541	4/1997	Albanese et al.	380/42
5,621,794	4/1997	Matsuda et al.	380/20
5,621,799	4/1997	Katta et al.	380/20
5,625,693	4/1997	Rohatgi et al.	380/23
5,684,876	11/1997	Pinder et al.	380/37

Primary Examiner—Stephen C. Buczinski

Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman

[57] **ABSTRACT**

Basic transfer units (BTUs) of compressed video data of video images are selectively encrypted in accordance with an encryption policy to degrade the video images to at least a virtually useless state, if the selectively encrypted compressed video images were to be rendered without decryption. As a result, degradation that approximates the level provided by the total encryption approach is achieved, but requiring only a fraction of the processor cycle cost required by the total encryption approach, to decrypt and render the video images.

19 Claims, 6 Drawing Sheets